



Disaster Preparedness: How to Develop a Business Continuity Plan

By Marc Berenfeld, CPA*

*Regulated by the State of Florida

Marc Berenfeld, CPA, is a senior partner with Berenfeld, Spritzer, Shechter & Sheer in Coral Gables, Fla. With 22 years' experience in audit, accounting, tax compliance, tax consulting, litigation support and financial management services, Marc oversees the firm's audit department, serving public and privately held companies in South Florida and throughout the United States. Marc is co-author of several articles, brochures and continuing education presentations offered through the Florida Institute of CPAs.



The Numbers Speak for Themselves

According to the National Federation of Independent Businesses, a University of Texas study estimates that more than half of small- and mid-size businesses (SMBs) that lose their data in a disaster go out of business within two years after that disaster. Another survey conducted by the U.S. National Archives and Records Administration found that 25 percent of companies experiencing an IT outage of two to six days went bankrupt immediately.

No business – and especially no accounting firm – wants to accept those kinds of risks.

Yet, the fact of the matter is that most businesses don't develop a disaster recovery plan until it's too late. Like most business development and major IT projects, a business continuity plan requires an investment of time and resources. Business leaders looking for the greatest return on their investment tend to put off business continuity until disaster strikes – a critical mistake that can jeopardize a business's survival.

Accounting firms make this mistake as well. In fact, it wasn't until after we experienced a business disruption that Berenfeld Spritzer committed the resources required to put a business continuity plan in place.

When Hurricanes Katrina and Wilma passed over South Florida in 2005, we were among the more fortunate businesses in the area, but we still lost 14 days of operations and revenue. While our data remained secure and intact, we realized that we needed to implement a business continuity plan and upgrade the technology infrastructure to support it. As a result, business continuity quickly moved up on our "to do" list.

While 2005's record-breaking hurricane season became the impetus for our business continuity plan – and considering that Hurricane Dean is, at this writing, bearing down on the Caribbean and Mexico – it is important to note that natural disasters represent only a small fraction of potential threats to business survivability. Businesses like ours contend daily with the threat of data losses; human error or malfeasance; systems failure; and viruses, worms or other malware. A comprehensive business continuity plan that could protect us from these threats was necessary in ensuring our business survives every day of the year, not only during hurricane season.

That same year, we had just over 50 professional associates in the firm, but plans – which were met – called for 100 by the end of the year and more than 150 by the end of 2006. Our company's growth necessitated a larger headquarters; the prospect of a new office presented a rare opportunity to build a new powerful, scalable state-of-the-art network that could support the business continuity plan.

Five Steps to the Plan

As he assessed the firm's needs, Berenfeld Spritzer's new IT director, Benjamin Thaw, turned to technology solutions provider CDW to provide valuable expertise and guidance.

Recognizing the scope of the requirements, CDW suggested the following five steps toward developing a comprehensive business continuity plan:

- 1. Conduct a business impact assessment.** This involved a cross-functional team to evaluate the business requirements and tier data based on the importance to our business operations.
- 2. Take steps to protect data.** It was important to back up data frequently to ensure records are kept, so we needed to upgrade our backup equipment to a faster version to reduce the time it took to complete a backup cycle.
- 3. Review power options.** We needed to add uninterrupted power supplies (UPS) for critical servers, network connections and selected personal computers to keep the most essential applications running in case of a power outage.
- 4. Document, test and update the disaster preparedness plan.** Part of Berenfeld Spritzer's plan needed to include updated configuration diagrams of the hardware, software and network components to be used in the recovery. The plan also needed to include logistical details, such as travel to backup sites and spending authorization for emergency needs.
- 5. Consider telecommunications alternatives.** Often taken for granted, telecommunications backup involving redundancy and alternatives needed to be in place – and in the case of spot outages, redundancy may be enough. For larger outages, alternative communications vehicles, including wireless phones, wireless data cards and satellite phones, had to be considered.

Once we understood the steps we needed to take to prepare a comprehensive business continuity plan, we developed a road map to help us get there. CDW also provided us with the expertise of the company's technology specialists in wireless, WAN/LAN, security, power and storage technologies to develop the plan.

"CDW's team provided immediate response and expedited shipments so that we could count on the delivery dates they set."

The Solution

The CDW specialty teams brought us comprehensive options and alternative approaches from virtually every manufacturer in the market, while providing guidance on which approach would work best for the firm based on our specific requirements and current IT plan. Within six months, Thaw and his team presented our partners with a comprehensive technology upgrade and business continuity plan. The IT program included:

- **Server Optimization:** In the data center, we went with six HP blade servers at the new headquarters in Coral Gables, consolidating from about 15 older servers.
- **Network Expansion:** The network backbone is based on Cisco Catalyst 4500 and 3750 switches, and includes 15 wireless access points firm wide.
- **Enhanced Storage:** The IT team chose HP's Modular Smart Array 1000 Storage Area Network (SAN), programmed to perform replication across the WAN.
- **Network Redundancy:** The Wide Area Network (WAN) is an MPLS Cloud running over dual, 3 Megabit T1 lines with redundant connections to Bell South.
- **Network Hardening:** The new network is protected by a layered solution that includes a RADIUS server appliance for network authentication; Web filtering; anti-virus through a spam filter and e-mail scanning; and a Citrix remote access application.
- **Power Management:** For power backup, we chose an American Power Conversion (APC) Symmetra PX 30-kilowatt, scalable to 40-kilowatts. Future plans include an expansion of power backup to 40 kilowatts, with a generator backup and distributed server capacity.
- **Document Management:** We implemented a company-wide document management system to ensure that important documents are classified, archived, updated when modified and retrievable under appropriate record retention policies. Combined with storage replication, this system protects the assets we create for our clients.

Our new network was in place, tested and waiting when we relocated our new headquarters over a single weekend. Employees shut off their computers in the old office on a Friday night and simply turned them on in the new building the following Monday morning.

Evaluation

The only issue we encountered during implementation was related to the proprietary software our firm uses, which is outsourced. Otherwise, all of these components integrated smoothly.

Having a trusted technology provider can make all the difference when making a major IT upgrade such as ours. CDW's team provided immediate response and expedited shipments so that we could count on the delivery dates they set. They arranged for vendors, such as our American Power Conversion (APC) representative, to be on hand during critical phases so that all of the pieces fit together. The UPS unit, for example, was ordered, delivered and installed entirely within just two weeks.

In the end, we found that the time and resources it took to upgrade our IT systems to support the business continuity plan improved our overall technology capabilities and the efficiency of our network.

More importantly, we now have the assurance of a functional business continuity plan to protect us against the hurricanes and tropical storms that threaten us six months out of every year. The protection we have against the daily threats of viruses, human error, malfeasance and systems failures that could result in data loss – threats common to businesses in every region – is just as critical in ensuring our firm's ability to survive.

Business continuity planning is an ongoing process that continuously requires the cooperation of the entire Berenfeld Spritzer team, with regular testing to ensure the plan functions properly. It is important for everyone within the organization to know what to do in the event of an emergency; regular testing of our business continuity system allows us to ensure our plan is complete, with no shortfalls. These business continuity essentials require a continued, dedicated investment of time and, ultimately, could mean the difference between failure and success.

When considering business continuity planning, it is important to remember that the process is similar to insurance. While it often seems like an exercise in futility before you need it, the risk of operating without it could mean business failure, and ultimately a loss of the time and resources it took to build your enterprise.

As with any significant business-essential operation, developing and implementing a reliable continuity plan takes time – normally the better part of a year – which is why the time to start is now, if you haven't done so already.